

**METHOD AND APPARATUS TO ELIMINATE THEFT OF ELECTRONIC  
EQUIPMENT USING EXISTING TELEPHONE JACK**

**FIELD OF THE INVENTION**

**[0001]** The present invention relates to methods and apparatus for inhibiting theft of electronic equipment.

**BACKGROUND OF THE INVENTION**

**[0002]** Electronic equipment found in offices and residential areas are valuable and therefore subject to theft. At present there exists a number of methods to inhibit the theft of electronic equipment. Traditionally, an anti-theft device will override the functioning of the equipment such as disrupting visual output or shutting down power as well as incorporate the use of an audible alarm upon detection of a theft. In many cases, the detection of theft in this manner does not aid in tracing the new location of the stolen equipment or in the identification of the apparent thieves.

**[0003]** In many existing anti-theft method and apparatus, the device itself requires that additional hardware be included to function properly. For example it is common to use added hardware needed to produce an audible alarm. Other devices such as that shown in US patent publication 2002/0108058 A1 to Iwamura, require a network to be present between the device being protected and a server, with this network further requiring a monitoring station to poll the protected devices. In addition, at present, electronic anti-theft devices override a device's operation or display requiring compatible software specific to the equipment being protected to control various functions of the equipment.

**[0004]** It is therefore an object of this invention to mitigate at least one of the above disadvantages in providing anti-theft protection to electronic equipment.

**SUMMARY OF THE INVENTION**

**[0005]** The present invention is based on the recognition that many modern electronic devices require connection to remote locations via telephone lines for the transfer of data and communication purposes.

1 [0006] The present invention provides a method and device to inhibit theft of electronic  
2 equipment using existing telephonic communication infrastructure. The device includes a  
3 microprocessor, which may be integrated into an electric circuit of the device to be protected,  
4 and a connection to a telecommunication module within the protected item that is used to  
5 communicate a message of apparent theft to an outside party. The microprocessor co-operates  
6 with the telecommunication module to transfer data indicative of the location of the device.  
7 From the data, a determination is made whether or not a theft has occurred.

8 [0007] Using the telephone connection, the method includes a set of steps in which it  
9 determines whether or not a theft has occurred and acts upon an indication of theft. In one  
10 embodiment, the steps include using an assigned password to configure the device to  
11 communicate wherein access allows the user to input the phone number that the protected device  
12 must be connected to for proper operation and the phone number of a security station or local  
13 police authority. Once set up, an automatic dialling of the equipment's own phone number  
14 occurs. The invention uses the response of this dialling in decision making. If the dialling  
15 results in a busy signal the device is in its proper location, if normal dialling occurs the device is  
16 no longer at its proper location and is therefore presumed stolen. If presumed stolen the second  
17 phone number is dialled to alert authorities of theft. To be executed upon dialling the second  
18 phone number, the device will access a pre-recorded message that is sent to the security station  
19 or police authority at the second phone number. The security station receives the message  
20 indicating that an apparent theft has occurred, and triggers a trace of the incoming call to detect  
21 the exact location of the stolen equipment. This exact location is used by the proper authority to  
22 retrieve the stolen equipment from the traced location.

23 [0008] Preferably, in addition to the above-mentioned steps, upon user input of the assigned  
24 password, a change can be made in data stored to accommodate a change of ownership or  
25 location of the protected equipment.

26

## 27 BRIEF DESCRIPTION OF THE DRAWINGS

28 [0009] These and other features of the preferred embodiments of the invention will become  
29 more apparent in the following detailed description in which reference is made to the appended  
30 drawings wherein:

- 1 [0010] Figure 1 shows schematically a residential installation.  
2 [0011] Figure 2 shows a functional block diagram of the anti-theft device.  
3 [0012] Figure 3 is a flow chart indicating operation of the component of Figure 2.

4

## 5 DESCRIPTION OF THE PREFERRED EMBODIMENTS

6

7 [0013] Referring therefore to Figure 1, an electronic component **D**, shown schematically as a  
8 television is located in a house **H**. The house **H** has an external phone line **L**, which through the  
9 existing infrastructure is connected to a security establishment **S**. It will be appreciated that the  
10 telephone link **L** may take any suitable form, including a wireless link or a cable connection.

11 [0014] Referring to Figure 2, an electronic component **D** includes an anti-theft device **7**. The  
12 device **7** includes a microprocessor **6** that is connected to an electric circuit **11** of the electronic  
13 component **7**. The microprocessor **6** is controlled by a software program **5**, which communicates  
14 with the storage areas **1,2,3,14** via data lines **4**. The storage areas typically in the form of data  
15 registers **1,2,3** contain information input by the user through an interface **9** and used to verify the  
16 operation of the component **7**. The remaining storage area typically in the form of a data register  
17 **14** contains information pre-loaded into the anti-theft device **7**. The program **5** also controls a  
18 telecommunication module **8**, which communicates through a phone line **10** connected by an  
19 external jack **13** to the external phone line **L**. A connection to the external jack **13** via the phone  
20 line **10** must be accomplished for the device **7** to allow operation of the equipment **D**.

21 [0015] The microprocessor **6** is responsive to a connection of power to the circuit to initiate  
22 an authentication procedure shown in Figure 3. Upon initial connection to a power supply and  
23 proper connection to an external jack **13**, the microprocessor **6** prompts the user to input a  
24 password to data register **1**. The register **1** may already be programmed to contain a password, in  
25 which case the user input is compared with the stored password, or may simply accept the initial  
26 input from the user and store it for future use. The interface then prompts the user for the phone  
27 number to which the device is connected, which it stores in register **2**, and the phone number of a  
28 security or police service **S** which it stores in register **3**.

29 [0016] Once the above initialization procedure is complete, the device **7** will resume normal  
30 operation unless prompted by the user via an interface **9** that the contents of data registers **2,3** are

1 to be changed. This normal operation will occur upon subsequent connections of the component  
2 to a power supply, after an interruption in power, provided the equipment **D** has been properly  
3 connected to the external jack 13. This ensures that in the event of a theft, the device 7 is  
4 capable of detecting the theft by continuing its normal operation while inhibiting a thief from  
5 changing the contents of data register 2 to the phone number of the new unauthorized location.  
6 Data register 1 can be accessed for comparison to a password input via an interface 9 in the event  
7 that the equipment being protected **D** lawfully changes locations or owners.

8 [0017] Again with reference to Figure 2, the software program 5 further to accessing the four  
9 data registers 1,2,3,14, communicates with the telecommunication module 8 of the protected  
10 equipment 7. The software program 5 using a timer, accesses the data lines 4 every thirty to  
11 sixty minutes first reading the contents of data register 2. It next sends this information via the  
12 data lines 4 to the equipment's telecommunication module 8 with instructions to dial the phone  
13 number via the telephone line 10 connected to an external jack 13. The data lines 4 receive the  
14 response of the dialling attempt through the telecommunication module 8 and carry this  
15 information back to the microprocessor 6, for the software program 5 to interpret the response.

16 [0018] Data register 2 containing the home phone number of the equipment to be protected **D**  
17 is utilised during normal operation. The software program 5 during intermittent security updates  
18 uses the information stored in register 2 to dial the number stored in data register 2 using the  
19 telecommunications module 8 and uses the response of this action to determine whether a theft  
20 has occurred. If the response is a "busy" signal, this indicates the security device 7 is connected  
21 to the proper telephone jack 13. If the signal dials and begins to ring, the equipment **D** is  
22 presumed to be stolen as it is not connected to the proper external jack 13. If stolen, the software  
23 program 5 accesses the contents of data register 3 and the pre-recorded message in data register  
24 14.

25 [0019] Data register 3 is designated to contain the phone number of the local police or  
26 security authority **S**. When the software program's 5 logic has determined a theft has occurred  
27 the software program 5 accesses its pre-recorded message 14 and the phone number stored in  
28 data register 3 and transfers these via the data lines 4 to the telecommunications module 8, where  
29 it is used to dial the assigned security organization **S**.

1 [0020] According to the logic explained above, if the response is interpreted as a theft, the  
2 software program 5 uses the data lines 4 to transfer the contents of data register 3 and the pre-  
3 recorded message 14 back to the telecommunication module 8 to be dialled. The  
4 telecommunication module 8 dials the number and sends the pre-recorded message 14 to the  
5 security station S. The security station S receives the pre-recorded message 14, which  
6 determines that an apparent theft has occurred and a trace begins on the incoming call. Once this  
7 operation is complete, the location of the stolen equipment D can be determined by the security  
8 organization S and passed on to the proper authority to retrieve the equipment D using the call  
9 placed via the telephone line 10 connected to an external jack 13. It can be appreciated that the  
10 device 7 may contact the police authority directly with its pre-recorded message 14, if a security  
11 organization S is not used.

12 [0021] Further to the above embodiments, again referring to Figure 2, the software program  
13 5 allows for manipulation of data register 2 and data register 3 in the event of change of  
14 ownership or location. When the microprocessor 6 receives input of its password via the data  
15 lines 4 and through an interface 9, the software program 5 compares this input to the contents of  
16 data register 1. If access is granted, the software program 5 allows the user to change the phone  
17 numbers stored in the above mentioned data registers 2,3 to prevent false alarms when the  
18 location of the protected equipment 7 is lawfully changed. Furthermore, it is required that a  
19 proper connection to an external jack 13 be made for the equipment being protected 7 to operate.  
20 This feature ensures that the device 6 will be able to properly detect a theft.

21 [0022] Although the invention has been described with reference to certain specific  
22 embodiments, various modifications thereof will be apparent to those skilled in the art without  
23 departing from the spirit and scope of the invention as outlined in the claims appended hereto.  
24  
25